(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENT- UND MARKENAMT

(12) **Offenlegungsschrift**

(10) **DE 198 32 950 A 1**

(21) Aktenzeichen: 198 32 950.4
(22) Anmeldetag: 22. 7. 98
(43) Offenlegungstag: 12. 8. 99

(51) Int. Cl.[6]:
B 60 T 13/66
B 60 T 8/88
B 60 T 17/22
B 60 Q 9/00
B 60 K 41/20

(66) Innere Priorität:
198 04 933. 1 07. 02. 98

(71) Anmelder:
ITT Mfg. Enterprises, Inc., Wilmington, Del., US

(74) Vertreter:
Blum, K., Dipl.-Ing., Pat.-Ass., 65779 Kelkheim

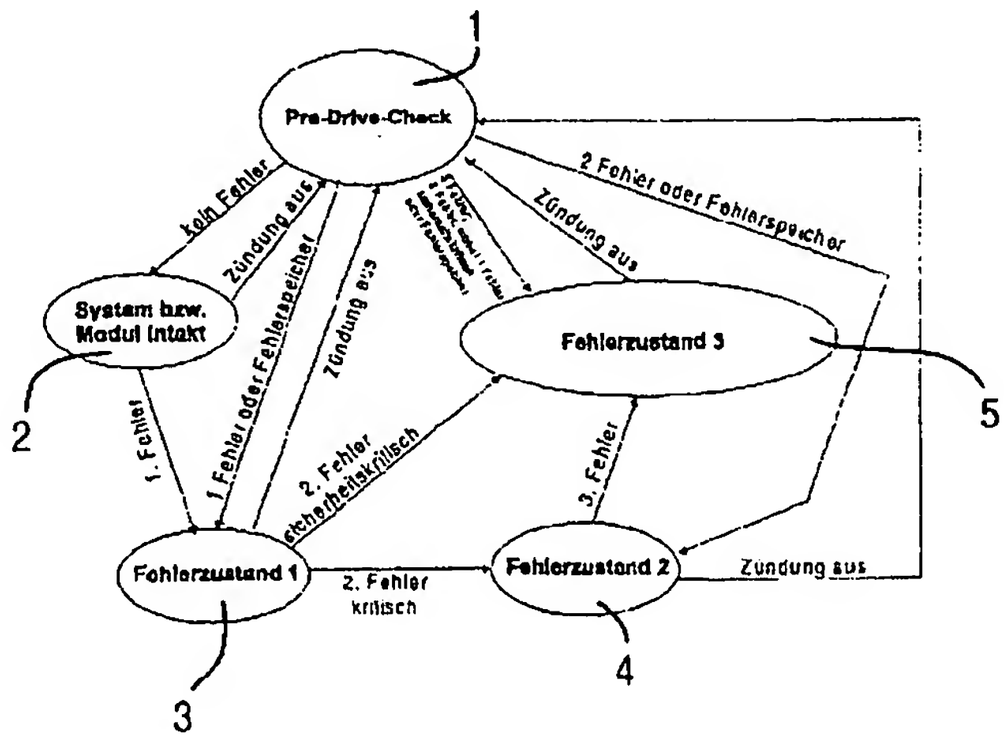
(72) Erfinder:
Böhm, Jürgen, Dr., 65558 Oberneisen, DE; Stölzl, Stefan, 69469 Weinheim, DE; Willimowski, Peter, 63486 Bruchköbel, DE; Hoffmann, Oliver, 65843 Sulzbach, DE; Nell, Jaochim, 63454 Hanau, DE; Oehler, Rainer, 64285 Darmstadt, DE

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

Rechercheantrag gem. Paragraph 43 Abs. 1 Satz PatG ist gestellt

(54) Verfahren zur Behandlung von Fehlern in einem elektronischen Bremssystem und zugehörige Vorrichtung

(57) Elektronische Bremssysteme stellen ein sicherheitskritisches verteiltes Echtheitssystem dar, an das hohe Anforderungen bezüglich der Fehlererkennung und -behandlung gestellt werden.
Die Erfindung beschreibt ein Verfahren und eine zugehörige Vorrichtung zur Behandlung von Fehlern in derartigen Systemen, das nur wenige definierte Systemzuszände (1 bis 5) zuläßt, unter Einschluß eines Pre-Checks (1), wobei der Übergang von einem Systemzustand in den nächsten Zustand nur durch Eintreten ganz bestimmter definierter Ereignisse erfolgen kann.



DE 198 32 950 A 1

Beschreibung

Die Erfindung bezieht sich auf ein Verfahren zur Behandlung von Fehlern in einem elektronischen Bremssystem von Fahrzeugen.

Die Erfindung betrifft ferner eine Vorrichtung zur Behandlung von Fehlern in einem elektronischen Bremssystem von Fahrzeugen, das mindestens einen Zentralrechner zur Ansteuerung der Radbremsen abhängig von dem Bremswunsch des Fahrers und dem Betriebszustand des Bremssystems aufweist, der einen Error Handling Code für die Fehlerbearbeitung aufweist.

Bremsanlagen für Kraftfahrzeuge werden immer komplexer. Das Antiblockiersystem (ABS), die Traction Control und Fahrzeugstabilisierungssysteme beispielsweise verlangen individuelle Bremseingriffe für einzelne Räder. Der Fahrer merkt dies beispielsweise durch das Pulsieren (Rubbeln) des Bremspedals bei der ABS-Regelung, was vom Fahrer nicht immer als angenehm empfunden wird und zu Fehlreaktionen führen kann.

Abhilfe schafft eine mechanische Entkopplung von Radbremsbetätigung und Bremspedal. Letzteres sorgt über geeignete Sensoren nur noch für die Erfassung des Fahrer-Bremswunsches, der elektrisch an die Bremsen weitergeleitet wird. Systeme, die eine derartige Entkopplung aufweisen, sind als "Brake-By-Wire-Systeme" bekannt geworden und sind beispielsweise in der DE-Z "ATZ Automobiltechnische Zeitschrift 98 (1996) 6. Seiten 328–333. in der US-5,230,549 und in der EP O 467 112 B1 beschrieben. Die unterste Ebene eines derartigen, typischerweise modular aufgebauten Systems, bilden vier intelligente Radbrems-Module. Sie regeln ein gefordertes Radbremsmoment radindividuell ein und stellen für das Gesamtsystem sozusagen universelle intelligente Aktuatoren dar. Sie bestehen aus einem Microcontroller (Slave) für die Regelung, einem Servoverstärker und der eigentlichen elektromechanischen Radbremse. Diese unterste Ebene bildet das sogenannte Radbremsmanagement.

Die mittlere Ebene ist für das Bremsmanagement des Gesamtfahrzeuges zuständig, beispielsweise für eine situationsspezifische Verteilung der Bremskräfte auf die einzelnen Radbremsen. Die Hardware dieser mittleren Ebene des Fahrzeugbremsenmanagements besteht aus einem zentralen Rechner (Master), der typischerweise aus Gründen der Ausfallsicherheit durch einen zusätzlichen Rechner für die Systemkontrolle überwacht wird.

Die oberste Ebene eines derartigen Brake-by-wire-Systems stellt die Schnittstelle zum Fahrer dar. Sie besteht typischerweise aus der Nachbildung eines konventionellen Bremspedales mit redundant ausgeführter Sensorik zur Erfassung des Fahrer-Bremswunsches und zusätzlichen Überwachungselementen, die verschiedene Fehlerzustände dieses sogenannten Pedalmoduls anzeigen können. In dem Pedalmodul erfolgt auch eine Vorverarbeitung der Sensorsignale. Auch dieses Pedalmodul kann einen eigenen Microcontroller aufweisen.

Die einzelnen Ebenen werden durch definierte logische Schnittstellen und typischerweise über ein echtzeitfähiges Bussystem, das vorzugsweise redundant ausgeführt ist, datenmäßig miteinander verbunden und gewährleisten daher eine optimale Modularität des Systems.

Beide Bussysteme (bzw. ggf. auch nur ein Bussystem) können auch durch normale analoge Leitungen ersetzt werden.

Als weitere zentrale Komponente eines modular aufgebauten Bremssystems ist das Powermanagement, die Energieversorgung, zu nennen.

Das Brake-by-Wire-System stellt ein sicherheitskritisches verteiltes Echtzeitsystem dar, an das hohe Anforderungen bezüglich der Fehlererkennung und Fehlerbehandlung gestellt werden.

Da der Fahrer keinen direkten Durchgriff auf die Bremse hat, muß das Bremssystem in jedem Fehlerfall mindestens eine Notfunktion aufrechterhalten, was in bekannter Weise durch eine fehler-aktive, funktionelle Redundanz gewährleistet wird. Weiterhin sollen die Systeme in bekannter Weise eine leistungsfähige On-Line-Diagnose besitzen, die auftretende Fehler auf jeden Fall erkennt, damit eine entsprechende Notfunktion aktiviert und der Fahrer gewarnt werden kann.

Diese Forderungen haben entscheidende Auswirkungen auf die Gestaltung der Energieversorgung, der zentralen Bremsregelung und auch der Warnstrategie des elektronischen Bremssystems.

Die Ausfallsicherheit der Energieversorgung wird in bekannter Weise (durch vorgenannte DE-Z) durch Einführung eines Tandembordnetzes gewährleistet. Bei Ausfall eines Teilsystems bleibt die Funktionsfähigkeit der im ausgefallenen Kreis gespeisten Komponenten bedingt erhalten.

Für einen sicheren Betrieb des Fahrzeugbremsenmanagemets (Regel- und Kontrollfunktionen) muß ein auftretender Fehler sowohl registriert als auch dessen Quelle erkannt werden. Deshalb ist daher gemäß einer bekannten Strategie in jedem Falle eine überwachende Einrichtung in dieser Ebene erforderlich. Das Hinzuziehen von Plausibilitätskriterien und geeigneten kontinuierlich ablaufenden Prüfroutinen innerhalb der Software stellen Maßnahmen dar, mit deren Hilfe Fehlerzustände lokalisiert und entsprechende Notfunktionen aktiviert werden.

So ist es aus der zitierten DE-Z bekannt, die Überprüfung der Rechner des Systems (Master und Slaves) mit Hilfe eines Kontrollrechners durchzuführen. Dabei werden sämtliche Rechner mit den wichtigsten Daten (Fahrerbremswunsch, Fahrgeschwindigkeit, Bremsmomente, etc.) versorgt und können durch Plausibilitätsbetrachtungen die Berechnungen der anderen Rechner überprüfen.

Bei Fehlfunktion des Masters oder des Kontrollrechners können die Slaves dies diagnostizieren und auf eine Notfunktion der Bremsanlage ohne Beteiligung des Masters umschalten.

Fehlfunktionen eines Slaves können vom Master und Kontrollrechner erkannt werden. Der Slave kann dann stillgelegt werden und die Notfunktion der restlichen Radbremsen wird nicht beeinträchtigt.

Durch die DE 195 10 525 A1 sind ferner Maßnahmen bekannt geworden, die die vorg. elektronischen Bremsanlagen mit Blick auf mögliche Fehlerzustände im Bereich der Bremswunscherfassung verbessern. Fehlersignale werden dabei über das Fahrzeugbremsenmanagement dem Radbremsenmanagement mitgeteilt, das radindividuelle Maßnahmen veranlaßt.

Die vorgenannten bekannten Maßnahmen gewährleisten jedoch noch kein umfassendes optimiertes Sicherheitskonzept.

Für ein umfassendes Sicherheitskonzept in dem entsprechenden Fehlerbehandlungs-System ist es notwendig, sämtliche Fehler des elektronischen Bremssystem zu erfassen und ihre Auswirkungen auf die jeweiligen Fahrsituationen zu berücksichtigen. Bei Anwendung der bekannten Konzepte würde dies dazu führen, eine Vielzahl von verschiedenen Zuständen des Bremssystems in die Sicherheitsbetrachtungen einschließen zu müssen, wodurch das System sehr komplex würde. Je komplexer jedoch das System aufgebaut ist, desto anfälliger wird es für Fehler, die dann zu Ausfällen von Komponenten des elektronischen Bremssystems führen können. Auch wird es schwierig, eine Rekonfiguration des

Bremssystems nach Auftreten eines Fehlers vorzunehmen.

Ferner ist im bekannten Fall keine systematische Strategie in der Behandlung der Zustände beim Auftreten von Mehrfachfehlern gegeben.

Der Erfindung liegt die Aufgabe zugrunde, das eingangs bezeichnete Verfahren so zu führen bzw. die Vorrichtung so auszubauen, daß die Anzahl der verschiedenen Zustände des elektronischen Bremssystems, in denen sich das System bei der Fehlererfassung und -behandlung befindet, so klein wie möglich gehalten werden kann und die Zustände dabei genau definiert sind.

Die Lösung dieser Aufgabe gelingt gemäß der Erfindung für das Verfahren mit dem Schritten:

- Festlegen und Definieren einer kleinen Anzahl von eindeutigen technischen Betriebszuständen des Bremssystems mit Vorgabe von bestimmten, definierten technischen Ereignissen, die allein einen Übergang von einem Betriebszustand in den nächsten Zustand bewirken,
- Verknüpfen der technischen Betriebszustände mit zustandsspezifischen Steuer-/Regelmaßnahmen sowie Warnmaßnahmen für den Fahrer des Fahrzeuges, und
- Erfassen von Fehlern im Bremssystem beim Start des Fahrzeuges durch einen Pre-Drive-Check und online beim Betrieb des Fahrzeuges und Durchführen einer entsprechend den Betriebszuständen fehlerzustandsabhängige Fehlerbehandlung.

Hinsichtlich der Vorrichtung gelingt die Lösung der Aufgabe ausgehend von der eingangs bezeichneten Vorrichtung dadurch, daß

eine kleine Zahl von eindeutigen technischen Betriebszuständen des Bremssystems festgelegt und definiert ist, mit Vorgabe von bestimmten technischen Ereignissen, die allein einen Übergang von einem Betriebszustand in den nächsten Zustand bewirken,
- er die technischen Betriebszustände zustandsspezifisch mit Steuer-/Regel-/ bzw. Warneinrichtungen für den Fahrer verbindet, und
- der Error Handling Code eine Pre-Drive-Check-Routine zur Erfassung von Fehlern im Bremssystem beim Start des Fahrzeuges und on-line beim Betrieb des Fahrzeuges aufweist, die entsprechend den Betriebszuständen eine fehlerzustandsabhängige Fehlerbehandlung durchführt.

Durch die erfindungsgemäßen Maßnahmen befindet sich das modular aufgebaute elektronische Bremssystem bei Auftreten eines oder mehrerer Fehler immer in einem genau definierten Zustand. Die Anzahl der verschiedenen Zustände ist dabei sehr klein, wodurch das System mit Vorteil nicht zu komplex wird und daher maßgebend weniger für Fehler anfällig wird, die zu Ausfällen von Systemkomponenten führen könnten. Durch die erfindungsgemäßen Maßnahmen ist daher immer genau bekannt, in welchem definierten Zustand sich das System gerade befindet. Dadurch ist es ohne weiteres möglich, eine Rekonfiguration des Bremssystems nach Auftreten eines Fehlers vorzunehmen.

Vorzugsweise werden auch unbenutzte Speicherplätze bei den Rechnern RAMs, ROMS, usw. auf einen definierten Wert gesetzt, damit man auch insoweit zu jeder Zeit weiß, in welchem Zustand sich das System, auch sein Speicherbereich, sich befindet.

Bei der Erfindung erfolgt ferner der Übergang von einem definierten Zustand in den nächsten definierten Zustand nur durch Eintreten ganz bestimmter definierter Ereignisse, was

sich ebenfalls entscheidend auf die Fehlersicherheit des Systems auswirkt.

Das erfindungsgemäße Verfahren mit den definierten Systemzuständen und den definierten Übergängen kann sowohl (vorzugsweise) für elektromechanische Bremsanlagen, aber auch generell für elektronisch unterstützte Bremssysteme verwendet werden.

Die Erfindung gewährleistet somit eine fehlerzustandsabhängige Fehlerbehandlung in einem Brake-by-Wire-System.

Gemäß einer Weiterbildung der Erfindung wird dieses Verfahren zur Behandlung von Fehlern in einem modular aufgebauten elektronischen Bremssystem mit nachfolgenden Schritten durchgeführt:

- Festlegen und Definieren einer kleinen Zahl von eindeutigen technischen Betriebszuständen des betreffenden Moduls mit Vorgabe von bestimmten, definierten technischen Ereignissen, die allein einen Übergang von einem Betriebszustand des Moduls in den nächsten Zustand bewirken,
- Verknüpfen der technischen Betriebszustände des Moduls mit zustandsspezifischen Steuer-/Regel-/Melde- bzw. Warnmaßnahmen, und
- Erfassen von Fehlern in dem jeweiligen Modul beim Start des Fahrzeuges durch einen Pre-Drive-Check und on-line beim Betrieb des Fahrzeuges und Durchführen einer entsprechend dem Modul-Betriebszuständen fehlerzustandsabhängige Fehlerbehandlung.

Bei der zugehörigen Vorrichtung, die neben dem Zentralrechner an Modulen autarke Unterrechner mit Error Handling Codes aufweist, sind die autarken Unterrechner so organisiert, daß

- eine kleine Zahl von eindeutigen technischen Betriebszuständen des jeweiligen Moduls festgelegt und definiert ist, mit Vorgabe von bestimmten technischen Ereignissen, die allein einen Übergang von einem Betriebszustand in den nächsten Zustand bewirken,
- sie die technischen Betriebszustände zustandsspezifisch mit Steuer-/Regel-/ bzw. Warneinrichtungen für den Fahrer verbinden, und
- der Error Handling Code eine Pre-Drive-Check-Routine zur Erfassung von Fehlern im Bremssystem beim Start des Fahrzeuges und on-line beim Betrieb des Fahrzeuges aufweist und entsprechend den Betriebszuständen eine fehlerzustandsabhängige Fehlerbehandlung durchführt.

Durch diese Weiterbildung der Erfindung wird somit an den betreffenden Modulen eine Eigendiagnose' sozusagen eine modulinterne Fehlerdiagnose, durchgeführt, was den Zentralrechner des Bremssystems wesentlich entlastet.

Weitere Merkmale und Vorteile der Erfindung ergeben sich anhand von in den Zeichnungen dargestellten Ausführungsbeispielen.

Es zeigen:

Fig. 1 ein grundlegendes Zustandsdiagramm für ein Brakeby-Wire-System mit definierten Übergängen,

Fig. 2 das Zustandsdiagramm des Brake-by-Wire mit definierten Übergängen für das gesamte Bremssystem,

Fig. 3 das Zustandsdiagramm des Bremspedalmoduls mit definierten Übergängen,

Fig. 4 das Zustandsdiagramm jeweils eines Radmoduls mit definierten Übergängen, und

Fig. 5 das Zustandsdiagramm der Energieversorgung mit definierten Übergängen.

Die **Fig.** 1 zeigt das erfindungsgemäße Zustandsdiagramm für ein Brake-by-Wire-System mit ganz definierten, wenigen technischen Systemzuständen und mit definierten technischen Übergängen zwischen den einzelnen Systemzuständen.

Das Zustandsdiagramm nach **Fig.** 1 gilt dabei sowohl für das Gesamtsystem als auch für entsprechende Unter-Systeme der einzelnen Module des Brake-by-Wire-Systems, wenn dieses gemäß einer bevorzugten Ausführungsform so aufgebaut ist, daß jedes Modul mit einem eigenen Untersystem ausgerüstet ist, das eine Intelligenz aufweist, um autark auch die Fehler in dem zugehörigen Modul zu erfassen und darzustellen. Dadurch wird die zentrale Fehlerbehandlung entlastet und braucht sozusagen nicht den einzelnen Fehler in den Modulen "hinterherzugehen". Sie erhält vielmehr von dem autarken Unter-System vollständige Statusmeldungen über den Fehlerzustand des betreffenden Moduls. Die Fehler in den einzelnen Modulen werden dabei mit bekannten Methoden online erfaßt.

Für das betrachtete Gesamtsystem, sowie die das Gesamtsystem darstellende Unter-Systeme der Module sieht die Erfindung vorzugsweise folgende, maximal fünf Zustände, die in **Fig.** 1 mit entsprechenden Bezugszeichen versehen sind, vor:

1. Pre-Drive-System-Check (PSC) bzw. Pre-Drive-Module-Check (PMC),
2. Bremssystem intakt,
3. Fehlerzustand 1,
4. Fehlerzustand 2 und
5. Fehlerzustand 3.

Die Übergänge zwischen den Zuständen **1** bis **5** sind mit den Pfeilen gekennzeichnet. Das Eintreten eines Übergangs erfolgt nur, wenn die Ereignisse an den Übergängen eintreten, wie sie an den Pfeilen in **Fig.** 1 beschrieben sind.

Der Pre-Drive-System-Check bzw. die Pre-Drive-Module-Checks gemäß Zustand **1** beinhalten Testroutinen mittels eines Error-Handling Codes in den jeweiligen System-Rechnern, die beim Starten des Fahrzeuges (Zündung an) oder beim Betätigen des Bremspedals (Bremslichtschalter) erfolgen. Nach einer Diagnose entscheidet der Check, ob das Bremssystem und die einzelnen Module intakt sind, oder ob ein bestimmter Fehlerzustand vorhanden ist. Entsprechend dieser Diagnose gehen die Module bzw. das gesamte Bremssystem gleich in den entsprechenden Zustand **2** oder **3, 4, 5** über. Dieser Pre-Drive-Check ist besonders bei einer Bremsanlage vom Brake-by-Wire-Typ sinnvoll, da es sich hierbei um eine Fremdkraftbremsanlage ohne mechanische Rückfallebene handelt. Bei einem rein hydraulischen Bremssystem ist eine aktive Überwachung und Diagnose nicht ohne weiteres zu realisieren.

Bei dem Pre-Drive-System-Check können beispielsweise durch einen Error Handling Code im Zentralrechner alle Bremsen kurz angesteuert und überprüft werden, ob alle Sensorsignale und entsprechende Statusmeldungen vorhanden sind. Als Alternative werden vor allem Module des Bremssystems und evt. von der Energieversorgung die Ergebnisse der individuellen Pre-Drive-Module-Checks abgefragt bzw. empfangen. Diese Funktionalität kann vorzugsweise im Zentralrechner implementiert werden. Je nach dem Zustand des gesamten Bremssystem hat der Zentralrechner sofort die Möglichkeit entsprechende Maßnahmen zu ergreifen. Bei Ausfall eines Radmoduls kann die Bremskraft z. B. sofort neu auf die noch intakten Module verteilt werden. Insgesamt kann die Funktionalität des Bremssystems entsprechend seinem aktuellen Zustand konfiguriert werden.

Da die restlichen Module ebenfalls im bevorzugten Fall mindestens einen Rechner besitzen, läuft auf diesen Modulrechnern jeweils ein separater Error Handling Code. Die gesamte Koordination dieser verschiedenen Error Handling Codes erfolgt vorzugsweise durch den Zentralrechner bzw. in dem Modul, in dem auch der Error Handling Code nach **Fig.** 1 abläuft. Als bevorzugte Ausführung hat jedes Modul einen eigenen Pre-Drive-Modul-Check. Mit dieser jeweils separaten Modul-Testroutine wird beim Starten des Fahrzeuges (Zündung an) oder beim Betätigen des Bremspedals (Bremslichtschalter) die Funktionsfähigkeit und der Zustand des Moduls überprüft.

Falls ein Modul keinen eigenen Rechner bzw. Elektronik hat, der den Pre-Drive-Modul-Check durchführen kann, so kann diese Testroutine von einem anderen Modul übernommen werden.

Befindet sich das Bremssystem in einem Fehlerzustand, so wird dieser Zustand in einem Fehlerspeicher abgespeichert, so daß das System beim nächsten Pre-Brake-Check sofort wieder in diesen Zustand übergeht, sofern nicht noch ein neuer Fehler aufgetreten ist, der dann das Bremssystem in einen anderen Fehlerzustand übergehen läßt. Der Zustand "Bremssystem intakt" wird dadurch nach Auftreten eines Fehlers beispielsweise erst dann wieder eingenommen, wenn das Bremssystem repariert worden ist.

Als Option bei dem Pre-Drive-System-Check bzw. dem Pre-Drive-Module-Checks kann eine Reset-Funktion für den Fehlerspeicher hinzugefügt werden. Falls während des Betriebs des Bremssystems ein Fehler aufgetreten ist, so wird dieser zunächst in dem Fehlerspeicher abgespeichert, der entweder zentral oder ebenfalls modular in den einzelnen Modulen realisiert werden kann. Beim nächsten Start des Fahrzeuges (Zündung an) wird der (oder die) Fehlerspeicher ausgelesen. Beinhaltet ein Fehlerspeicher den Fehlerzustand 2 bzw. Fehlerzustand 3 (Systemzustand **4** oder **5**), so wird zunächst dieser abgespeicherte Fehlerzustand nach den Checks eingenommen. Liegt im Fehlerspeicher der Fehlerzustand 2 vor und kommt ein weiterer Fehler bei den Pre-Drive-Checks hinzu, wird Fehlerzustand 3 eingenommen. Hingegen kann bei abgespeichertem Fehlerzustand 1 (Systemzustand **3**) die Reset-Funktion eingeführt werden. Das heißt, daß der Fehlerspeicher bei Fehlerzustand 1 gelöscht werden kann, wenn bei den Pre-Drive-Checks kein Fehler aufgetreten ist. Falls der Fehlerzustand 1 die Ansteuerung einer zugehörigen Warnlampe beinhaltet, so besteht hier die Möglichkeit, diese Warnlampe nicht unnötig lang anzusteuern.

Als Erweiterung des Fehlerspeichers kann die Anzahl des aufgetretenen 1. Fehlers mitgezählt werden. Wenn eine gewisse, vorher definierte Mindestzahl dieser aufgetretenen Fälle (1. Fehler während dem Betrieb und Reset bei den Pre-Drive-Checks) vorliegt, so kann die zugehörige Warnlampe angesteuert bleiben.

Die Fehlerzustände nach **Fig.** i sind vorzugsweise mit einer festgelegten gestuften Warnstrategie verknüpft, d. h. mit Warnstufen, die beim Erkennen verschiedener Fehler in dem elektronischen Bremssystem greifen sollten, d. h. mit einer bestimmten Ansteuerung verknüpft sind. In einem elektronischen Bremssystem können Fehler unterschiedlicher Kritikalität entstehen. Bei einem sich anbahnenden Totalausfall muß beispielsweise der Fahrer "gezwungen werden", das Fahrzeug mit geringer Geschwindigkeit, z. B. 30 km/h, aus dem Gefahrenbereich zu bringen und das Fahrzeug mit der Feststellbremse sicher abzustellen.

Es kennzeichnet der Fehlerzustand 1 (Systemzustand **3**) das Auftreten eines Fehlers, der nicht kritisch ist, weil er keinen wesentlichen Einfluß auf das Grund-Fahrverhalten hat und volle Grund-Bremssystemfunktion gewährleistet; ein Beispiel dafür ist der Ausfall des ABS-Systems.

Diesem Fehlerzustand 1 kann ein spezifischer, für den Fahrer bestimmtes Signal, zugeordnet werden, beispielsweise eine gelbe Warnlampe.

Der Fehlerzustand 2 (Systemzustand **4**) kennzeichnet das Auftreten eines kritischen Fehlers, der einen, wenn auch noch beherrschbaren, Einfluß auf die Fahrdynamik hat. Beispiel: Ausfall eines Kreises (Batterie) bzw. einer Bremse. Diesem Fehlerzustand wird ebenfalls ein spezifisches Signal zugeordnet, beispielsweise eine rote Warnlampe.

Der Fehlerzustand 3 (Systemzustand **3**) kennzeichnet das Auftreten eines überkritischen Fehlers, der Einfluß auf die Grundbremsfunktion hat, z. B. verringerte Leistungsfähigkeit der Radbremse wegen geringem Spannkraftniveau bzw. eines äußerst kritischen Fehlers, der auf einen baldigen Totalausfall der Bremsanlage hindeutet. Beispiel: Ausfall beider Batterien. Diesem Fehlerzustand wird ebenfalls ein spezifisches Signal zugeordnet, beispielsweise die rote Warnlampe gemäß dem Fehlerzustand 2 in Verbindung mit der Erzeugung eines akkustischen Warnsignals und/oder Reduzierung der maximalen Geschwindigkeit des Fahrzeuges auf einen fest eingestellten Wert, z. B. 50 km/h. Diese Geschwindigkeitsbegrenzung kann über eine Ansteuerung des E-Gas (bzw. Eingriff ins Motormanagement) erfolgen. Ferner ist es denkbar, daß eine Zeitmessung mit verwendet wird. Je länger das System nicht repariert wird, desto mehr wird die maximale Geschwindigkeit reduziert. Im einfachsten Fall kann Fehlerzustand 2 mit Fehlerzustand 3 gleichgesetzt werden und z. B. nur die rote Warnlampe ange-steuert werden, was allerdings für die Warnlampenstrategie dem heutigen Stand der Technik entsprechen würde.

Es wurde bereits dargestellt, daß zweckmäßig jeder Modul ein eigenes Rechnersystem besitzt, in dem jeweils eine zugeordnete Fehlerroutine implementiert ist. Die Zustandsdiagramme der einzelnen Module sind gleichartig zu dem des Systems nach **Fig.** 1 in den **Fig.** 2 bis 6 dargestellt und zeigen die einzelnen Zustände und die zugehörigen Übergänge.

Die **Fig.** 2 zeigt das Zustandsdiagramm für das gesamte Bremssystem. Der Pre-Braking-Check des Zustandes kann hier mit dem Pre-System-Check des Zustandes **1** in **Fig.** 1 gleichgesetzt werden. Die verschiedenen Zustände und Übergänge in **Fig.** 2, die denen der **Fig.** 1 entsprechen, werden vorzugsweise im Zentralrechner des elektronischen Bremssystems implementiert. Diese Funktionalität wird als "Error-Handling Code Zentral-rechner" bezeichnet.

Das Zustandsdiagramm für den Bremspedalmodul ist in **Fig.** 3 dargestellt.

Bei dem Bremspedalmodul beinhaltet der Pre-Pedal-Check des Zustandes **1** mindestens eine Überprüfung der Pedalsensorik und soweit möglich, einen Funktionstest der Auswerteelektronik für die Fahrerwunschgenerierung der Pedal-Elektronik und den Busanschlüssen.

Im übrigen entspricht das Zustandsdiagramm demjenigen nach **Fig.** 1.

Das Zustandsdiagramm für jedes Radmodul ist in **Fig.** 4 dargestellt. Jedes Radmodul überprüft bei seinem eigenen Pre-Radmodul-Check (Zustand **1**), ob z. B. im Fall einer elektronischen Bremse der Elektromotor angesteuert werden kann, die Bremsbeläge bewegt werden können und die Radmodulsensorik eine plausible Reaktion auf die Anregungen des Pre-Modul-Checks geben. Prinzipiell wird die Elektronik, Mechanik und Sensorik des Radmoduls so umfangreich wie möglich auf die Funktions-tüchtigkeit hin überprüft werden. Das Zustandsdiagramm für das Radmodul enthält, wie die **Fig.** 4 erkennen läßt, nicht den Fehlerzustand 2 und den Fehlerzustand 3, da auch bei Auftreten von mindestens zwei Fehlern innerhalb eines Radmoduls nur die gelbe Warnlampe angesteuert wird, wenn kein weiterer Fehler innerhalb des gesamten Bremssystems auftritt.

Das Zustandsdiagramm für das Bussystem ist in **Fig.** 5 dargestellt.

Beim Bussystem wird als eine bevorzugte Ausführungsform davon ausgegangen, daß das Bussystem redundant aufgebaut ist und zwei Bussysteme beinhaltet. Bei Ausfall eines Bussystems würde der Ausfall des zweiten Bussystems zu einem Totalausfall des gesamten Bremssystems führen. Deshalb muß dann sofort in den Fehlerzustand 1 (Zustand **3**) übergegangen werden.

Der Zustand **4** entfällt daher bei der Fehlerstrategie für das Bussystem.

Der Pre-Bus-Check (Zustand **1**) beinhaltet im wesentlichen eine Überprüfung, ob über das redundante Bussystem alle Teilnehmer angesprochen werden können und diese ein "Lebenszeichen" in Form einer Antwortnachricht geben.

Dieser Pre-Bus-Check kann auch von einem anderen Modul durchgeführt werden. d. h. es wird dann kein eigener Mikrocontroller für das Bussystem benötigt.

Das Zustandsdiagramm für die Energieversorgung des Bremssystems gemäß **Fig.** 6 nimmt eine gesonderte Stellung ein, da die Energieversorgung Bestandteil des Bremssystems ist. Eine redundant aufgebaute Energieversorgung kann beispielsweise im Fahrzeug generell den elektrische Fahrzeugaggregaten und somit auch dem Bremssystem zur Verfügung stehen. Das heißt, die Schnittstelle zwischen der Energieversorgung und dem Bremssystem kann beispielsweise durch zwei separate Versorgungsleitungen realisiert sein. Der Pre-Power-Check (Zustand **1** in **Fig.** 6) könnte sich dann beispielsweise auf eine Überprüfung der für das Bremssystem notwendigen Batterie-spannungsversorgung beschränken. In einer erweiterten Form werden zusätzlich die Ladezustände der Batterien überprüft, ob diese noch ausreichend für das Bremssystem sind.

Eine bevorzugte Realisierungsform der Energieversorgung hat nach Auftreten eines ersten Fehlers (z. B. Ausfall des Generators) den Übergang in Fehlerzustand 1 (Zustand **3**) und Ansteuerung der gelben Warnlampe zur Folge. In diesem Zustand muß der Batterieladezustand beider Batterien ständig überwacht werden. Wenn ein gewisser Mindestenergiegehalt einer Batterie unterschritten wird, ist in den Fehlerzustand 3 zu wechseln.

Die in den **Fig.** 2 bis 6 dargestellten Zustandsdiagramme sind bevorzugte Ausführungsbeispiele.

Prinzipiell kann ein einziges Modul die Funktionalität und Koordination aller Module übernehmen. Dann ist dieses Modul vorzugsweise fehlertolerant aufgebaut, damit eine Mehrheitsentscheidung im Fehlerfall möglich ist. Somit können in einer vereinfachten Ausführungsform alle Pre-Module-Checks und der Pre-System-Check in einem einzigen Modul erfolgen, beispielsweise dem des Zentralrechner. Fehlertolerant heißt, daß bei Auftreten eines Einfachfehlers in einem redundanten System der fehlerhafte Zweig durch eine Mehrheits-Entscheidungs-Logik erkannt wird, so daß der weiterhin funktionsfähige Zweig die Systemfähigkeit aufrechterhält, wodurch der erkannte Einfachfehler "toleriert" werden kann.

Für die Koordination der Übergänge zwischen den einzelnen Zuständen gibt es folgende bevorzugte Ausführungsform:

Jedes Modul macht seine eigene Koordination. Mindestens ein Modul macht die Koordination für das gesamte System.

Die Ansteuerung der Warneinrichtungen kann auf folgende Arten erfolgen:

1. Ein fehlertolerantes Modul übernimmt diese Aufgabe, das heißt, auch bei Eintreten eines Fehlers inner-

Nummer: DE 198 32 950 A1
Int. Cl.[6]: B 60 T 13/66
Offenlegungstag: 12. August 1999

FIG. 1

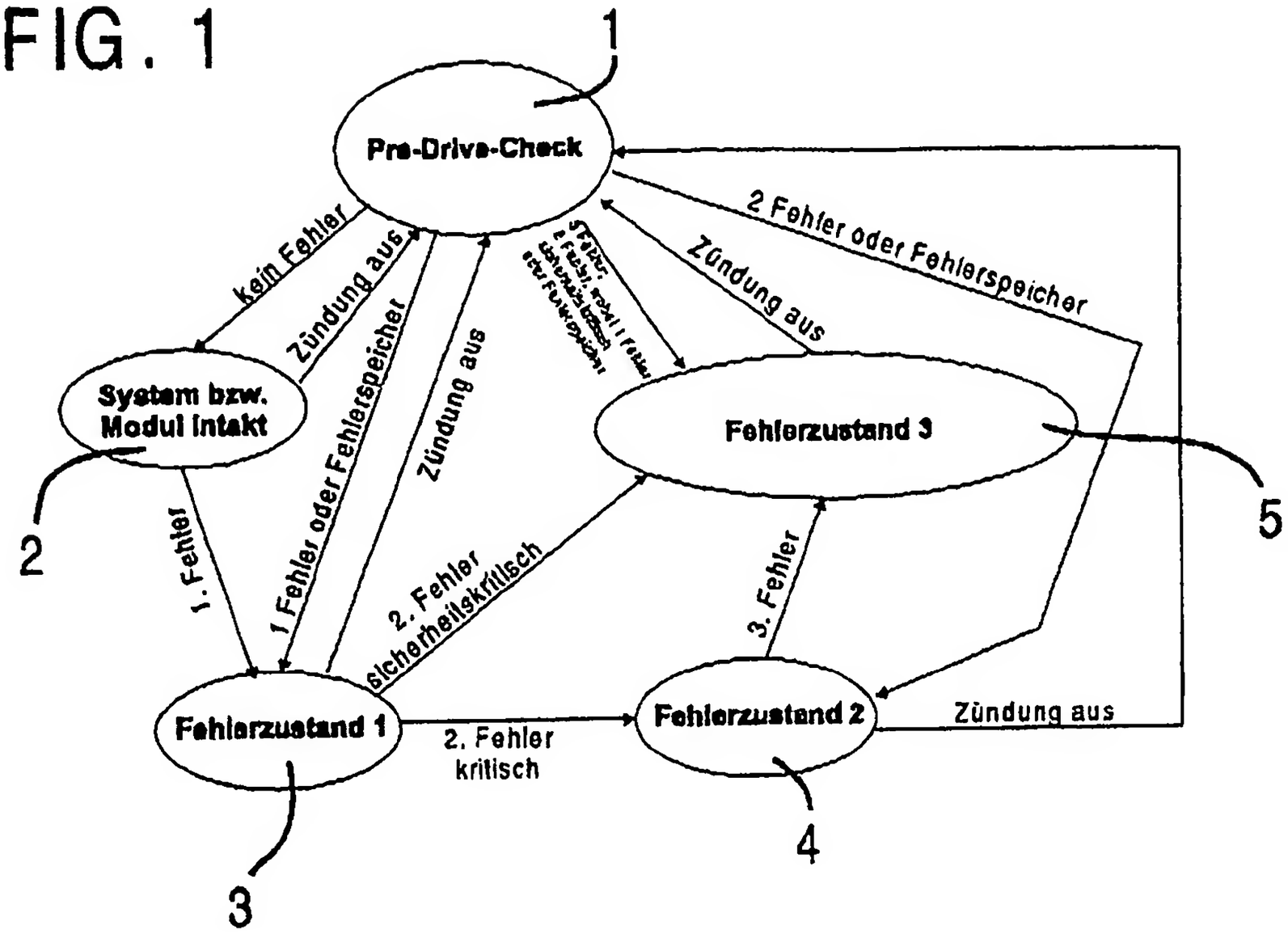
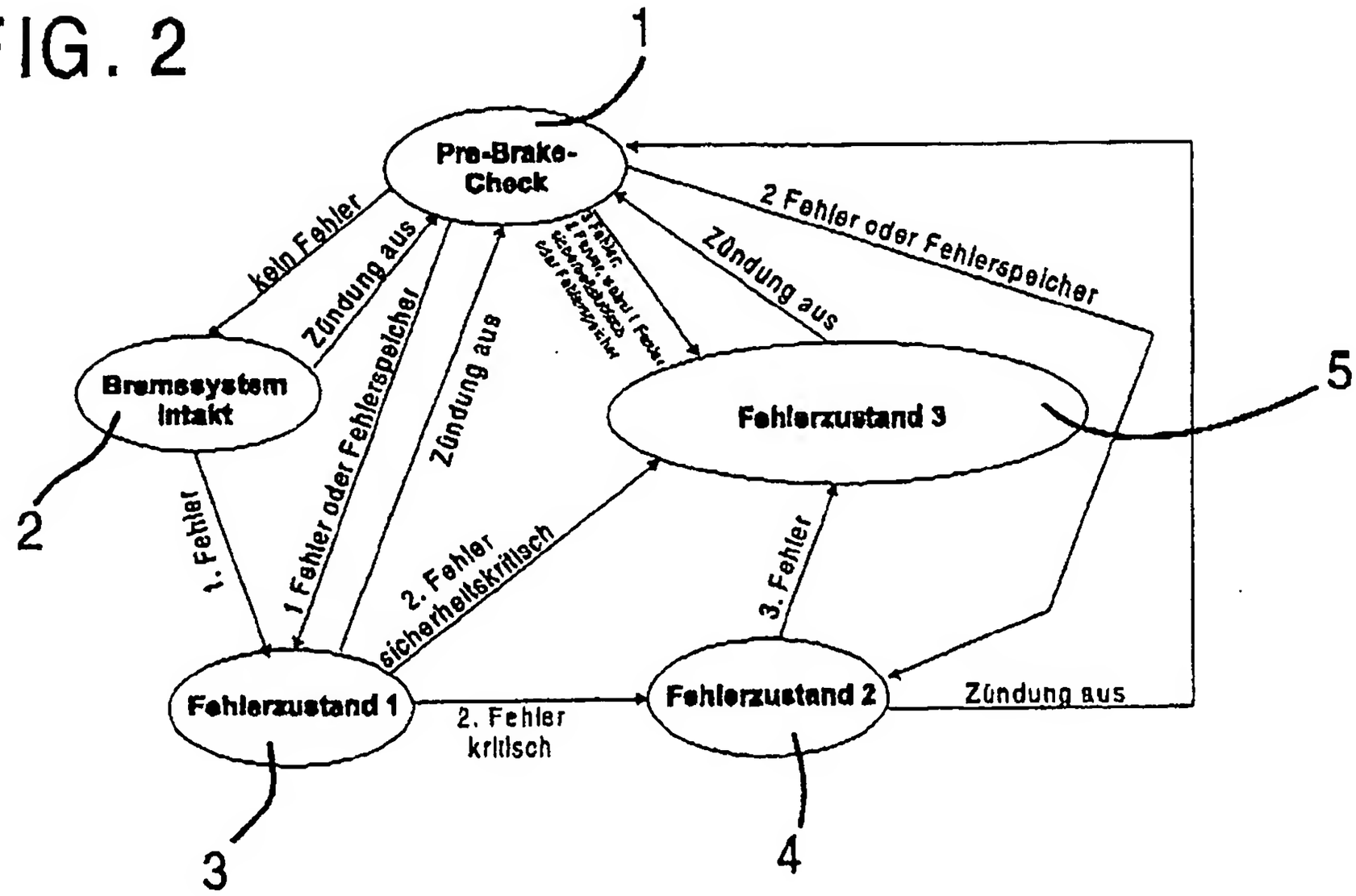


FIG. 2



Nummer: DE 198 32 950 A1
Int. Cl.[6]: B 60 T 13/66
Offenlegungstag: 12. August 1999

FIG. 3

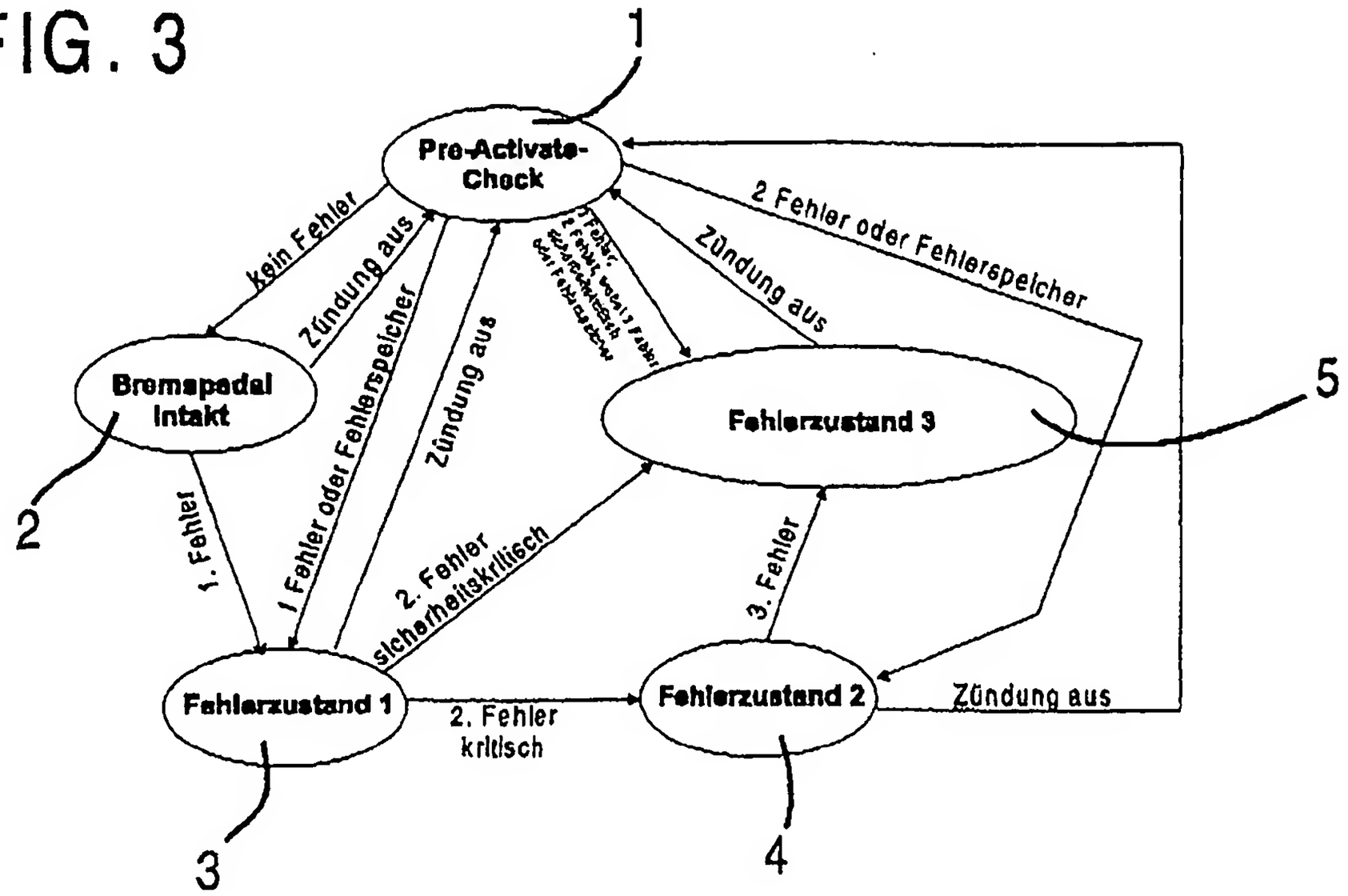
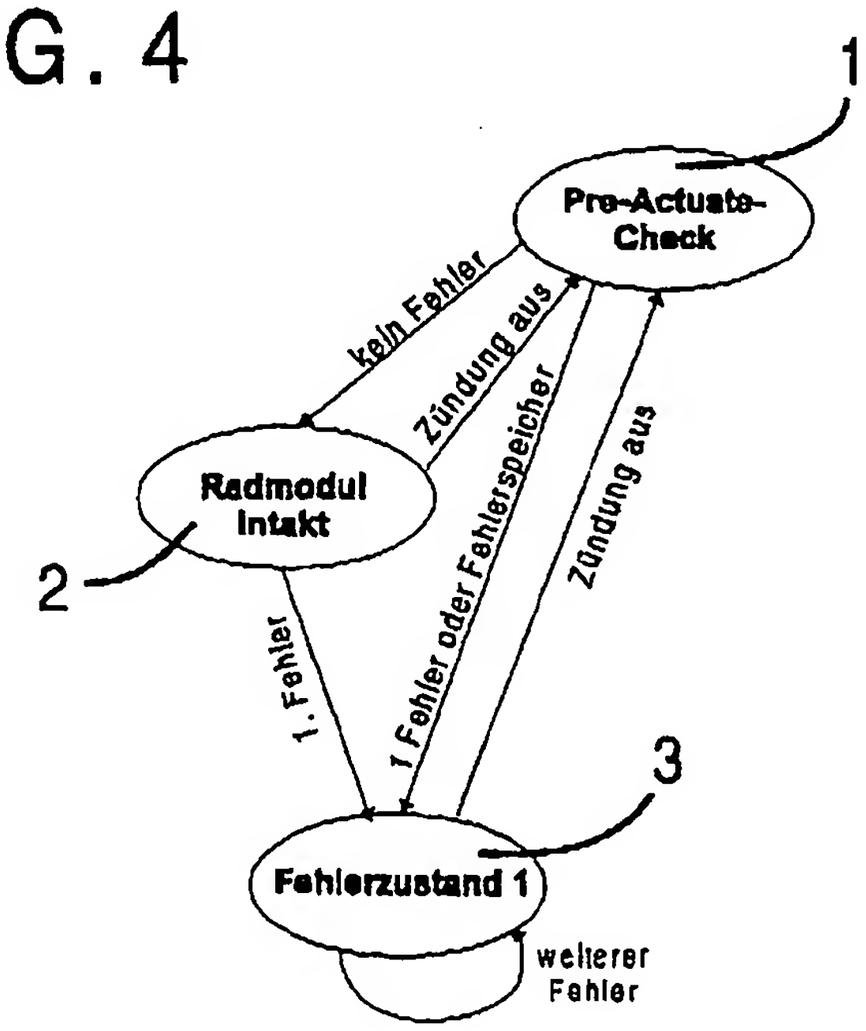


FIG. 4



Nummer: DE 198 32 950 A1
Int. Cl.[6]: B 60 T 13/66
Offenlegungstag: 12. August 1999

FIG. 5

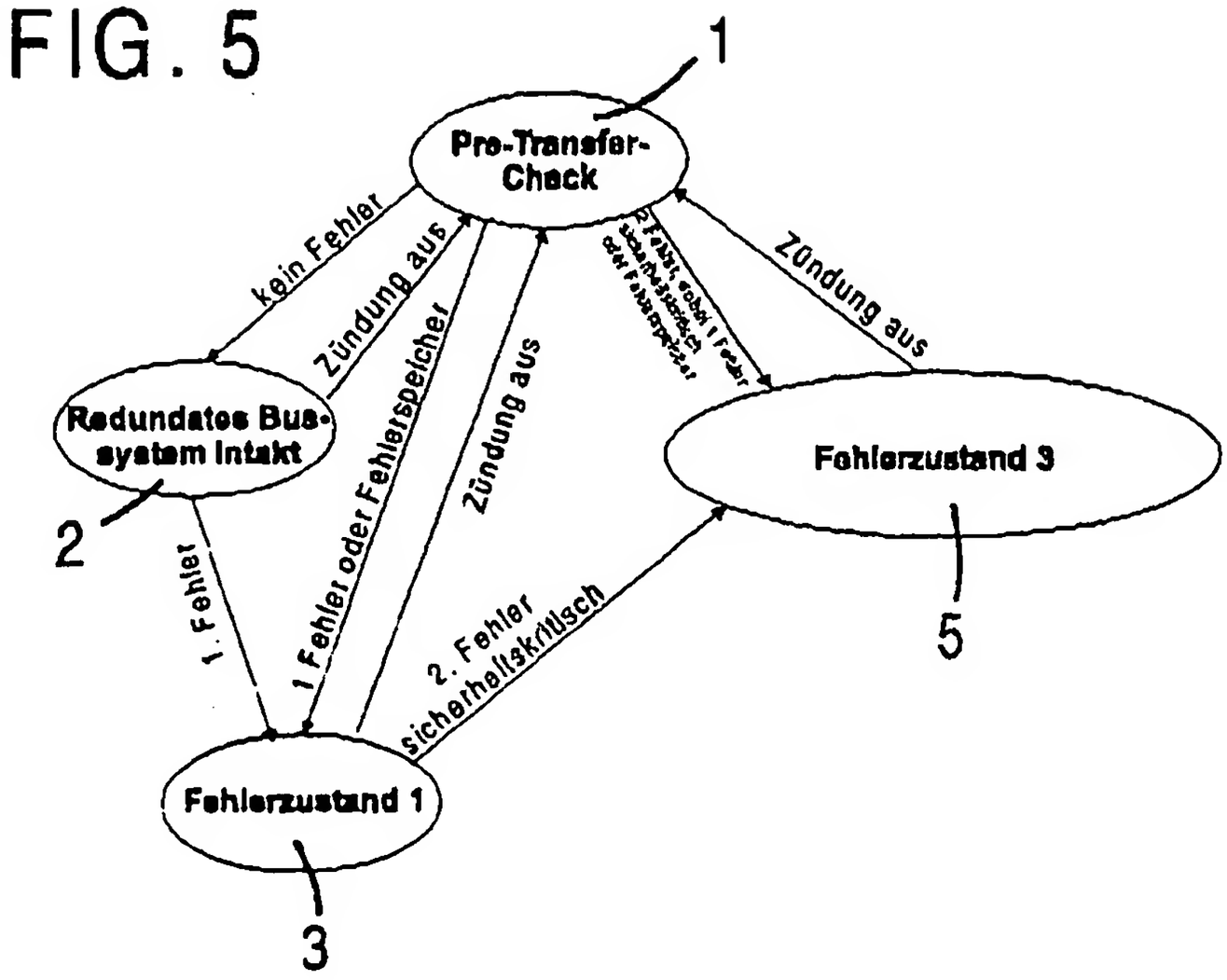


FIG. 6